

Listing of Claims (including amendments and status):

1 1. (Currently amended) An X.509 certificate stored on a computer readable medium for
2 interpretation execution on computer apparatus supporting reading of the certificate and control
3 of network cryptograpic operation according to the certificate , said certificate capable of
4 supporting more than one cryptographic algorithm with an associated public key, comprising:

5 a signature algorithm and signature for all authenticated attributes including a first public
6 key associated with a first cryptographic algorithm;

7 a first certificate extension identifying at least one alternative cryptographic algorithm
8 and providing a respective associated public key; and

9 a second certificate extension containing a signature for each alternative cryptographic
10 algorithm, whereby an alternative cryptographic algorithm may be supported without establishing
11 a new certificate hierarchy..

1 2. (Previously presented) An X.509 certificate according to Claim 1, wherein the first
2 cryptographic algorithm is RSA and the alternative cryptographic algorithm is elliptic curve and
3 the first and second certificate extensions are identified as non-critical.

1 3. (Previously presented) An X.509 certificate according to Claim 1, wherein the certificate can
2 be verified by either the signature for the first cryptographic algorithm or the signature for the
3 alternative signature algorithm.

1 4. (Currently amended) A method for enabling an X.509 certificate to support more than one
2 cryptographic algorithm, with associated public key, said method comprising the steps of:

3 providing the X.509 certificate with a signature algorithm with associated public key and
4 signature for all authenticated attributes using a first cryptographic algorithm;

5 providing the X.509 certificate with a first certificate extension identifying at least one
6 alternative cryptographic algorithm and providing a respective associated public key; and

7 providing the X.509 certificate with a second certificate extension which contains a
8 signature for each alternative cryptographic algorithm, whereby an alternative cryptographic
9 algorithm may be supported without establishing a new certificate hierarchy.

1 5. (Previously presented) A method for enabling an X.509 certificate to support more than one
2 cryptographic algorithm according to Claim 4, wherein the first cryptographic algorithm is RSA
3 and the alternative cryptographic algorithm is elliptic curve and the first and second certificate
4 extensions are indicated as non-critical.

1 6. (Previously presented) A method for enabling an X.509 certificate to support more than one
2 cryptographic algorithm according to Claim 4, wherein the certificate can be verified by either
3 the signature for the first cryptographic algorithm or the signature for the alternative signature
4 algorithm.

1 7. ((Previously presented) Computer readable code stored on computer readable media for
2 enabling an X.509 certificate to support more than one cryptographic algorithm in association
3 with a public key, said computer readable code comprising:

4 first subprocesses for providing the X.509 certificate with a signature algorithm and
5 signature for all authenticated attributes including a first public key using a first cryptographic
6 algorithm;

7 second subprocesses for providing the X.509 certificate with a first certificate extension
8 for identifying at least one alternative cryptographic algorithm and providing its associated public
9 key; and

10 third subprocesses for providing the X.509 certificate with a second certificate extension
11 which contains a signature for the alternative cryptographic algorithm.

1 8. (Previously presented) Computer readable code for enabling an X.509 certificate to support
2 more than one cryptographic algorithm according to Claim 7, wherein the first cryptographic
3 algorithm is RSA and the alternative cryptographic algorithm is elliptic curve and the first and
4 second certificate extensions are identified as non-critical.

1 9. (Previously presented) Computer readable code for enabling an X.509 certificate to support
2 more than one cryptographic algorithm according to Claim 7, wherein the certificate can be
3 verified by either the signature for the first cryptographic algorithm or the signature for the
4 alternative signature algorithm.

5 10. ((Previously presented) In a computing environment, a system for enabling an X.509
6 certificate to support more than one cryptographic algorithm, said system comprising:

7 means for providing the X.509 certificate with a signature for all authenticated attributes
8 including a first public key using a first cryptographic algorithm;

9 means for providing the X.509 certificate with a first certificate extension identifying at
10 least one alternative cryptographic algorithm and providing its associated public key; and

11 means for providing the X.509 certificate with a second certificate extension which
12 contains a signature for the alternative cryptographic algorithm.

1 11.(Previously presented) A system for enabling an X.509 certificate to support more than one
2 cryptographic algorithm according to Claim 10, wherein the first cryptographic algorithm is RSA
3 and the alternative cryptographic algorithm is elliptic curve and the first and second certificate
4 extensions are indicated as non-critical.

- 1 12. ((Previously presented) A system for enabling an X.509 certificate to support more than one
- 2 cryptographic algorithm according to Claim 10, wherein the certificate can be verified by either
- 3 the signature for the first cryptographic algorithm or the signature for the alternative
- 4 cryptographic algorithm.

Serial No. 09/240,265

5

Docket CR9-98-095